EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Overview

Plaintiff accuses Defendant of infringement through making, using, selling, offering for sale, and importation of Zoho's ("Defendant" or "Zoho") ManageEngine, including Endpoint Central and Vulnerability Manager Plus (the "Accused System and Method"), and all substantially similar products. The term "Accused System and Method" includes the associated computer hardware, interfaces, software, and data, and the processes and methods related thereto.

The Accused System and Method is accused of directly infringing U.S. Patent No. 10,075,466 (the"'466 Patent"). Plaintiff further accuses Defendant of indirectly infringing the '466 Patent by providing its customers and others the Accused System and Method to utilize in an infringing manner. Defendant intends to cause infringement by its customers and users as Defendant instructs users to use the Accused System and Method in an infringing manner. Defendant deploys client software to implement the Accused System and Method. Defendant also provides support and implementation services for the Accused System and Method, including providing instructions, guides, online materials, and technical support.

The asserted claims include elements that are implemented, at least in part, by proprietary electronics and software in the Accused System and Method. The precise designs, processes, and algorithms used in them are held secret, at least in part, and are not publicly available in their entirety. An analysis of Defendant's documentation and/or source code may be necessary to fully and accurately describe all infringing features and functionality of the Accused System and, accordingly, Plaintiff reserves the right to supplement these contentions once such information is made available to Plaintiff. Furthermore, Plaintiff reserves the right to revise these contentions, including as discovery in the case progresses, in view of the Court's final claim construction in this action and in connection with the provision of its expert reports.

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

10,075,466 Claim 1	Evidence
An apparatus, comprising: an intrusion prevention node configured to:	ManageEngine *an intrusion prevention node configured to* (e.g., The vulnerability information collected across multiple endpoints that are connected to the server) Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Intrusion detection and prevention** Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules. At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any. https://www.manageengine.com/security.html?mesearch

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

<table>
<tr>
<td></td>
<td>


https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html
</td>
</tr>
<tr>
<td>receive a result of at least one operation performed on at least one of a plurality of</td>
<td>ManageEngine receive a result of at least one operation performed on at least one of a plurality of networked devices (e.g., The vulnerability information collected by scanning operation) the at least one operation based on first information from at least one first data storage identifying a plurality of</td>
</tr>
</table>

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

networked devices, the at least one operation based on first information from at least one first data storage identifying a plurality of potential vulnerabilities including at least one first potential vulnerability and at least one second potential vulnerability, the at least one operation configured for:	*potential vulnerabilities* (e.g., emerging vulnerabilities) *including at least one first potential vulnerability and at least one second potential vulnerability* (e.g., Multiple vulnerability information collected from open source and stored in central database after verification and then system scan across multiple endpoints) Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Intrusion detection and prevention** Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules. At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any. https://www.manageengine.com/security.html?mesearch

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

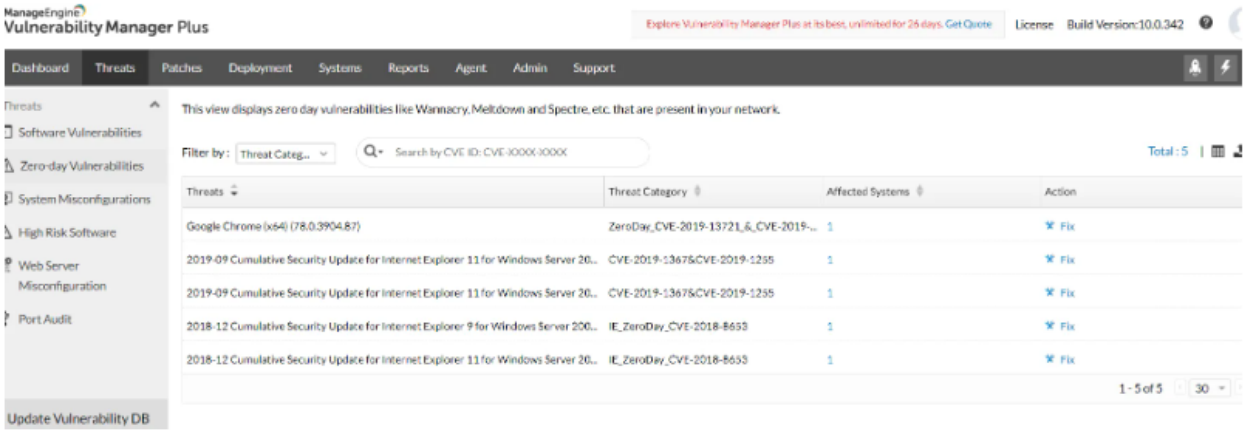
	Comprehensive vulnerability scanning Eliminating blind spots is the basis of successful vulnerability management. To achieve this, Vulnerability Manager Plus: • Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems. • Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move. • Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more. https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Leverage a dedicated view for zero-days

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.



Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. *Subscribe to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news*

https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Vulnerability Manager Plus Server:

The Vulnerability Manager Plus Server helps you to centrally perform all the vulnerability management and compliance tasks in your network endpoints. Some of the tasks include the following:

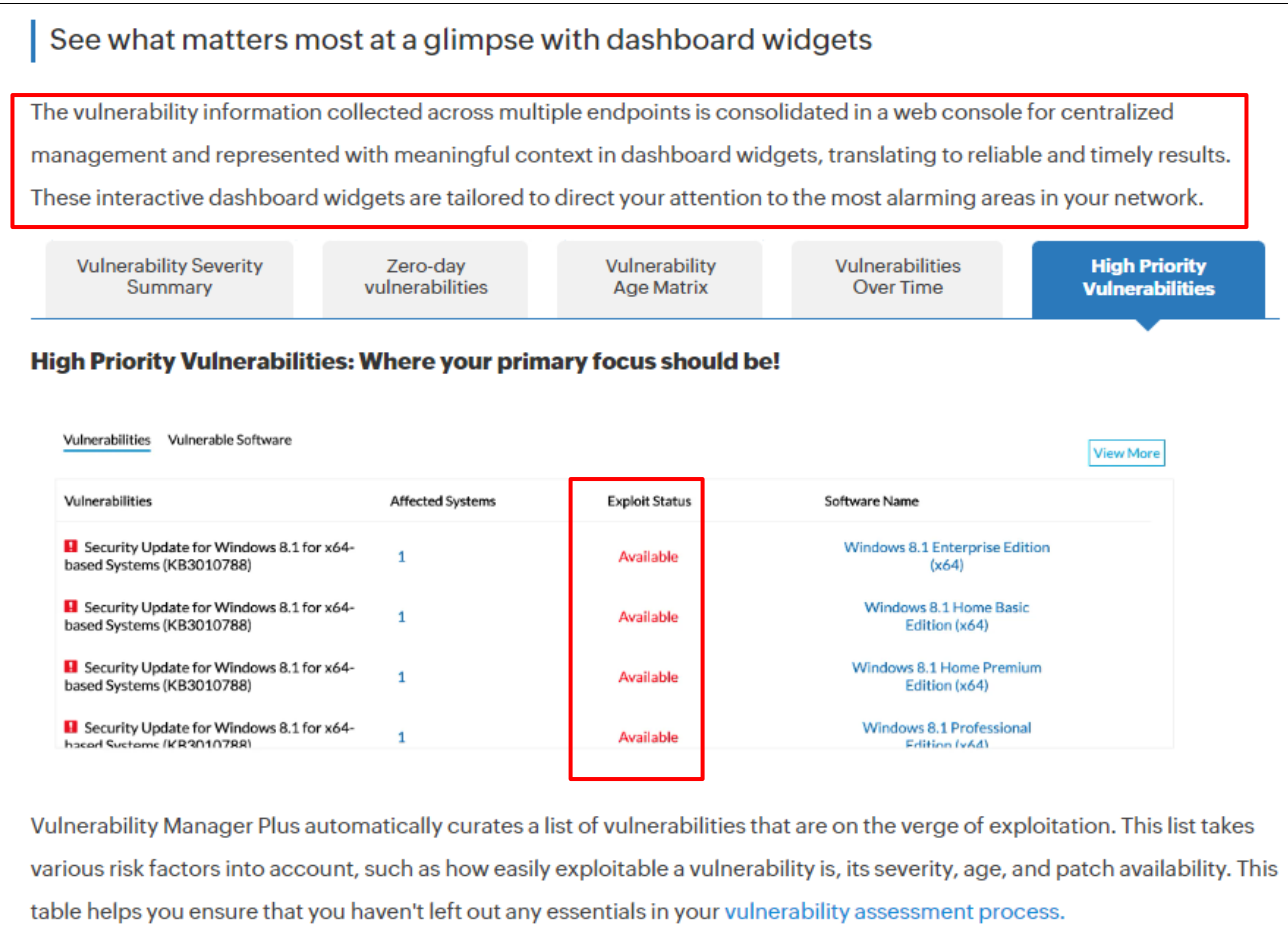
- Installing agents in computers
- Scanning computers for vulnerabilities and misconfigurations
- Deploying patches and secure configurations
- Uninstalling high-risk software
- Auditing active ports
- Auditing for compliance against CIS benchmarks

Any of the Windows computers in your network with the requirements mentioned here can be hosted as your Vulnerability Manager Plus Server. This Vulnerability Manager Plus Server at the customer site subscribes to the Central Vulnerability Database, from which it synchronizes the latest information on threats, patches, vulnerabilities, and compliance policies. Patches are downloaded directly from vendor sites and stored centrally in the server's patch store and will be replicated to your network endpoints to conserve bandwidth.

https://www.manageengine.com/vulnerability-management/help/vulnerability-management-architecture.html#v1

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

<table>
<tr>
<td></td>
<td>


https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html
</td>
</tr>
<tr>
<td>identifying at least one configuration associated with</td>
<td>ManageEngine identifying at least one configuration associated with the at least one networked device (e.g., The vulnerability information collected by scanning operation and identify a misconfiguration).</td>
</tr>
</table>

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

the at least one networked device, and	Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any): How to prevent security misconfigurations? If vulnerabilities are the gateway to the network, it's the misconfigurations that attackers leverage to worm their way to the intended targets. Security misconfigurations are not hard to fix, but they are unavoidable in an enterprise operating at scale. Finding them is a needle in the haystack, as they can be located across any component in an organization's systems, such as its servers, operating systems, applications, and browsers. Lack of visibility and centralized means to remediate misconfigurations makes organizations fall victim to misconfiguration attacks. https://www.manageengine.com/vulnerability-management/misconfiguration/?mesearch

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

	As soon as it's up and running in your network, Vulnerability Manager Plus automatically discovers your Active Directory and workgroup assets. Scaling up? No problem. Since Vulnerability Manager Plus is constantly in sync with Active Directory, new assets will be brought under management as soon as they enter your network, leaving no opportunity for new threats to go unnoticed. Leveraging endpoint agent technology, Vulnerability Manager Plus scans your laptops, desktops, servers, databases, workstations, and virtual machines across your entire global hybrid IT environment every 90 minutes, irrespective of whether they're within the corporate boundary or not. You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ. Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation. https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html
determining that the at least one networked device is actually vulnerable to at least one actual vulnerability, based on the identified at least one configuration and the first information from the	ManageEngine *determining that the at least one networked device is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration and the first information from the at least one first data storage identifying the plurality of potential vulnerabilities* (e.g., The vulnerability information collected by scanning operation and identify a misconfiguration based on vulnerability information collected from open source and stored in central database). *such that second information associated with the result is stored in at least one second data storage separate from the at least one first data storage* (e.g., The vulnerability information collected across multiple endpoints is consolidated in a

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

at least one first data storage identifying the plurality of potential vulnerabilities, such that second information associated with the result is stored in at least one second data storage separate from the at least one first data storage, the second information relating to the at least one actual vulnerability to which the at least one networked device is actually vulnerable;	web console for centralized management which is different from central database). *the second information relating to the at least one actual vulnerability to which the at least one networked device is actually vulnerable* (e.g., The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and if vulnerabilities exist then displays them in a dedicated view in the console with its fix) Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any): How to prevent security misconfigurations? If vulnerabilities are the gateway to the network, it's the misconfigurations that attackers leverage to worm their way to the intended targets. Security misconfigurations are not hard to fix, but they are unavoidable in an enterprise operating at scale. Finding them is a needle in the haystack, as they can be located across any component in an organization's systems, such as its servers, operating systems, applications, and browsers. Lack of visibility and centralized means to remediate misconfigurations makes organizations fall victim to misconfiguration attacks. https://www.manageengine.com/vulnerability-management/misconfiguration/?mesearch

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity Summary | Zero-day vulnerabilities | Vulnerability Age Matrix | Vulnerabilities Over Time | **High Priority Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities | Vulnerable Software — View More

Vulnerabilities	Affected Systems	Exploit Status	Software Name
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your vulnerability assessment process.

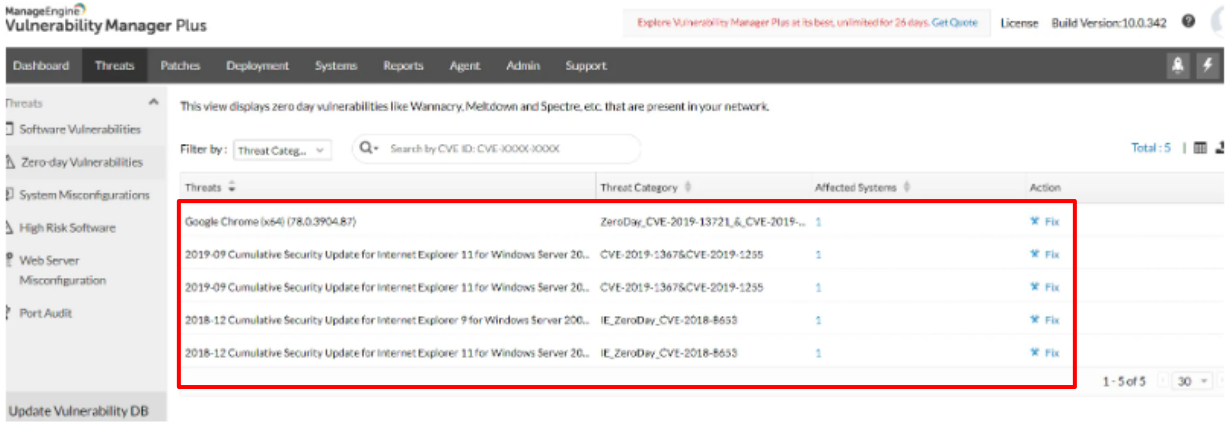
https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Leverage a dedicated view for zero-days

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.



Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network. Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. *Subscribe to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news*

https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

	How can I view the complete list of CVEs affecting my endpoints? Vulnerability Manager Plus boasts a dedicated Detected CVEs view that lists all the CVEs affecting your network endpoints. All you have to do is select the desired CVEs then click Fix CVE to instantly create a patch deployment task in all the affected machines. https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html As soon as it's up and running in your network, Vulnerability Manager Plus automatically discovers your Active Directory and workgroup assets. Scaling up? No problem. Since Vulnerability Manager Plus is constantly in sync with Active Directory, new assets will be brought under management as soon as they enter your network, leaving no opportunity for new threats to go unnoticed. Leveraging endpoint agent technology, Vulnerability Manager Plus scans your laptops, desktops, servers, databases, workstations, and virtual machines across your entire global hybrid IT environment every 90 minutes, irrespective of whether they're within the corporate boundary or not. You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ. Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation. https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

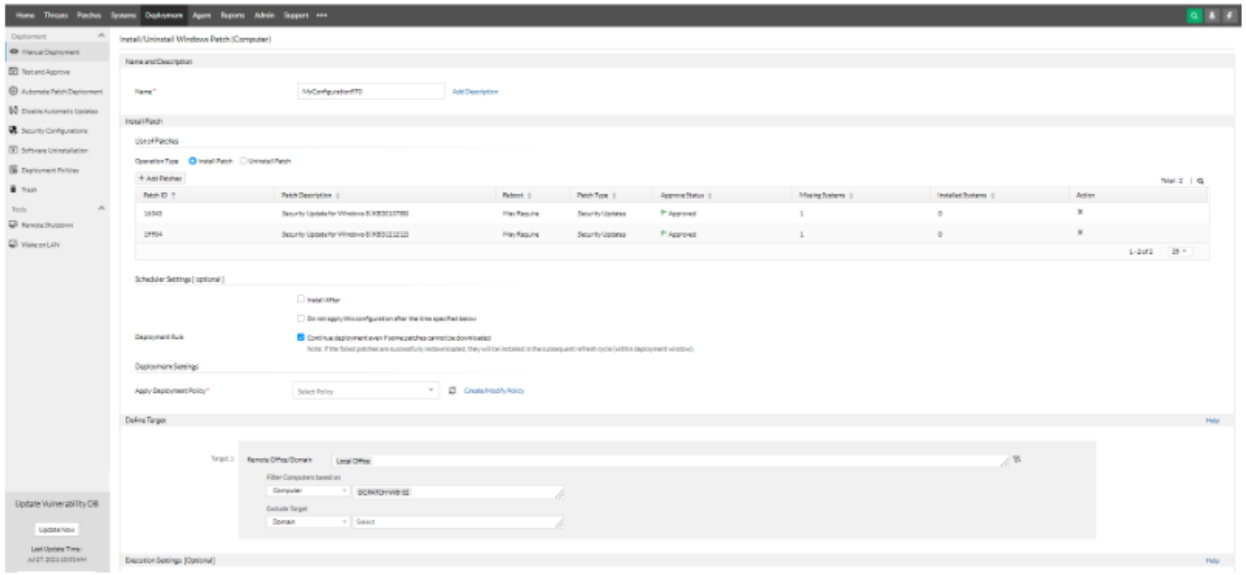
	Leverage built-in patching to ensure swift and accurate remediation With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.  https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html
cause display, via at least one user interface, a plurality of	ManageEngine *causes to display, via at least one user interface* (e.g., ManageEngine Vulnerability Manager Plus includes web consol) , *a plurality of techniques including a first technique for utilizing an*

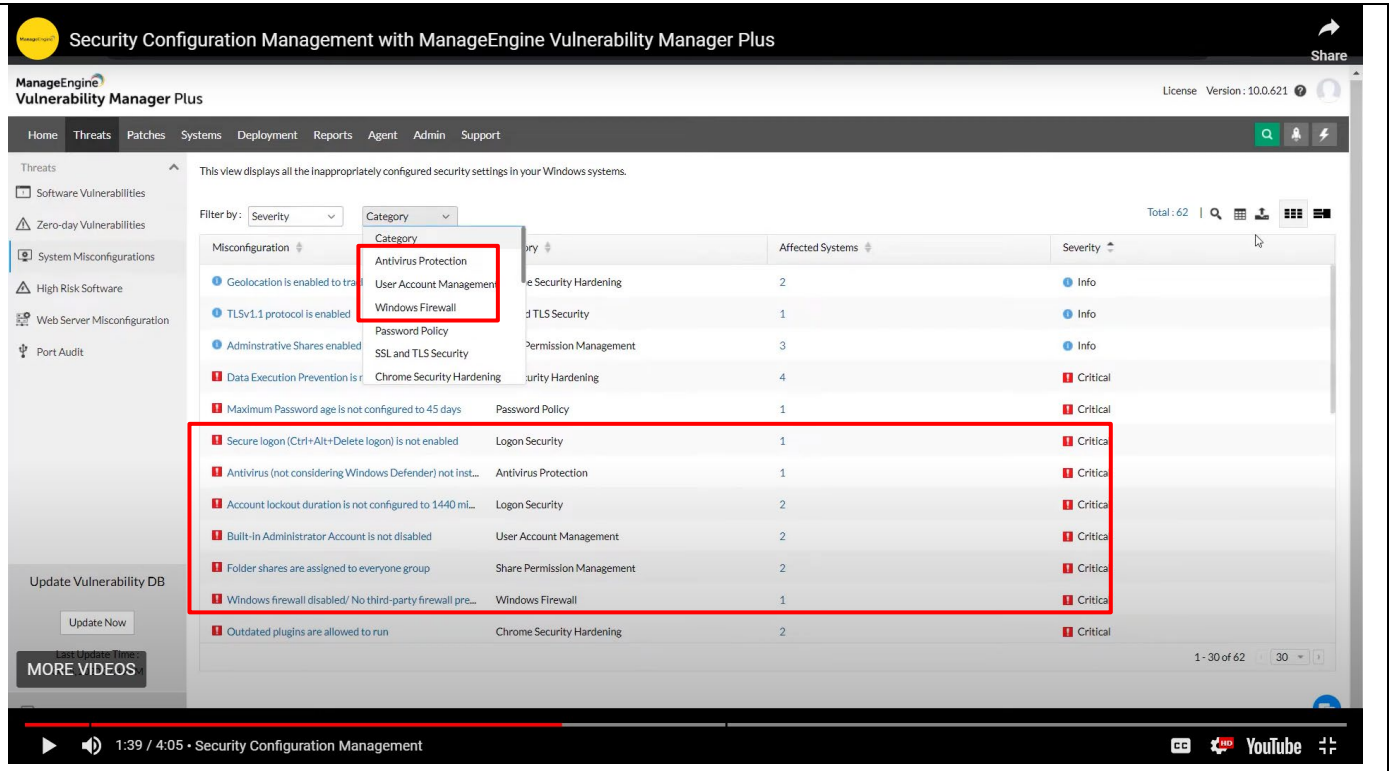
EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

techniques including a first technique for utilizing an intrusion prevention system component for occurrence mitigation, and a second technique for utilizing a firewall for occurrence mitigation;	*intrusion prevention system component for occurrence mitigation* (e.g., ManageEngine Vulnerability Manager Plus includes antivirus option), *and a second technique for utilizing a firewall for occurrence mitigation* (e.g., ManageEngine Vulnerability Manager Plus includes firewall option). The ManageEngine provides flexibility to choose the devices for applying the different policies or mitigation techniques according to the requirements. Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Intrusion detection and prevention** Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules. At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any. https://www.manageengine.com/security.html?mesearch

EXHIBIT 14

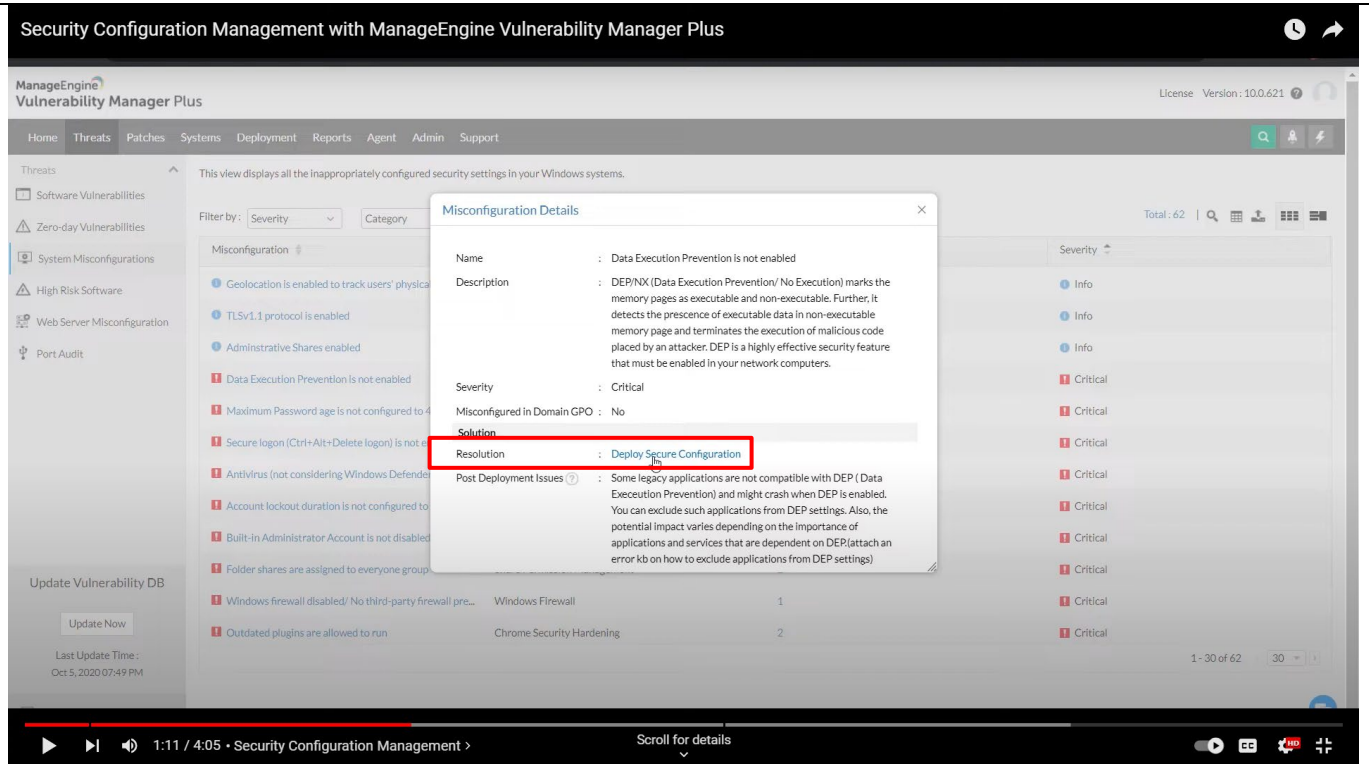
U.S. Patent No 10,075,466 v. Zoho



https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho



https://www.youtube.com/watch?v=p2Oh87NruMo&t=53s

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

	# Firewall Policy Management Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes. • Add, modify, and delete network and service objects • Add, modify, and delete firewall rules • Analyze the implications of proposed firewall rule changes • Push changes directly to the firewall Refer the 'Firewall Rule Administration' page for more details. Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for most major firewall devices including Cisco, FortiGate, WatchGuard, and Check Point. https://www.manageengine.com/products/firewall/firewall-rule-management.html

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

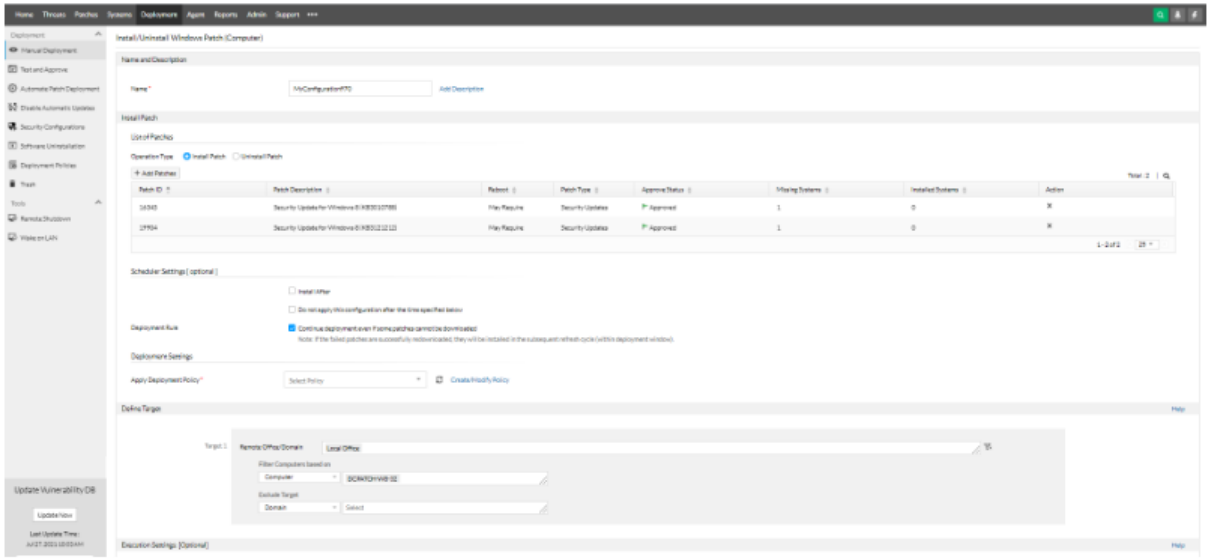
	Leverage built-in patching to ensure swift and accurate remediation With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.  https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html
allows receipt of:	ManageEngine *allows receipt , user input causing selection of the first technique for utilizing the intrusion prevention system component for occurrence mitigation* (e.g., ManageEngine Vulnerability Manager Plus

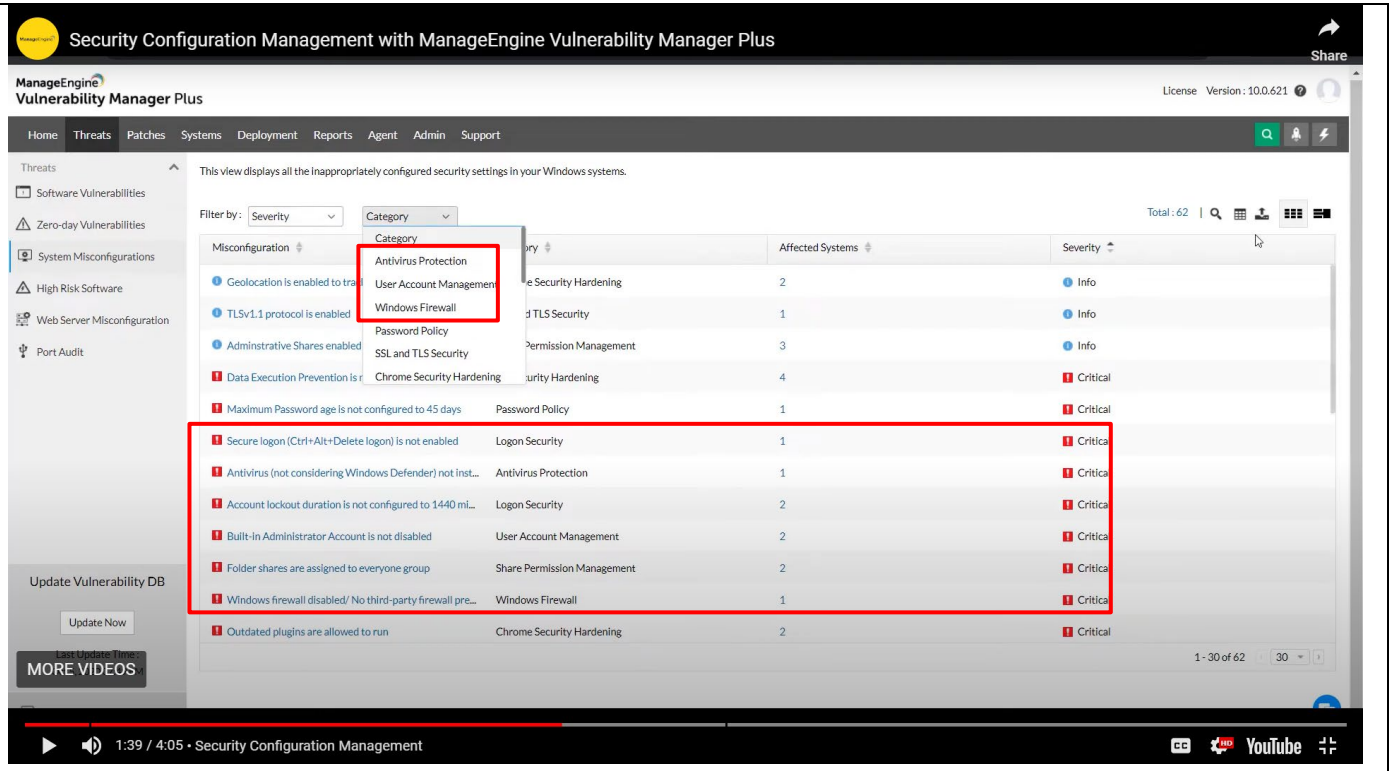
EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

user input causing selection of the first technique for utilizing the intrusion prevention system component for occurrence mitigation; user input causing selection of the second technique for utilizing the firewall for occurrence mitigation;	includes web consol on which user can select antivirus option) , *user input causing selection of the second technique for utilizing the firewall for occurrence mitigation* (e.g., ManageEngine Vulnerability Manager Plus includes firewall option). The ManageEngine provides flexibility to choose the devices for applying the different policies or mitigation techniques according to the requirements. Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Intrusion detection and prevention** Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules. At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any. https://www.manageengine.com/security.html?mesearch

EXHIBIT 14

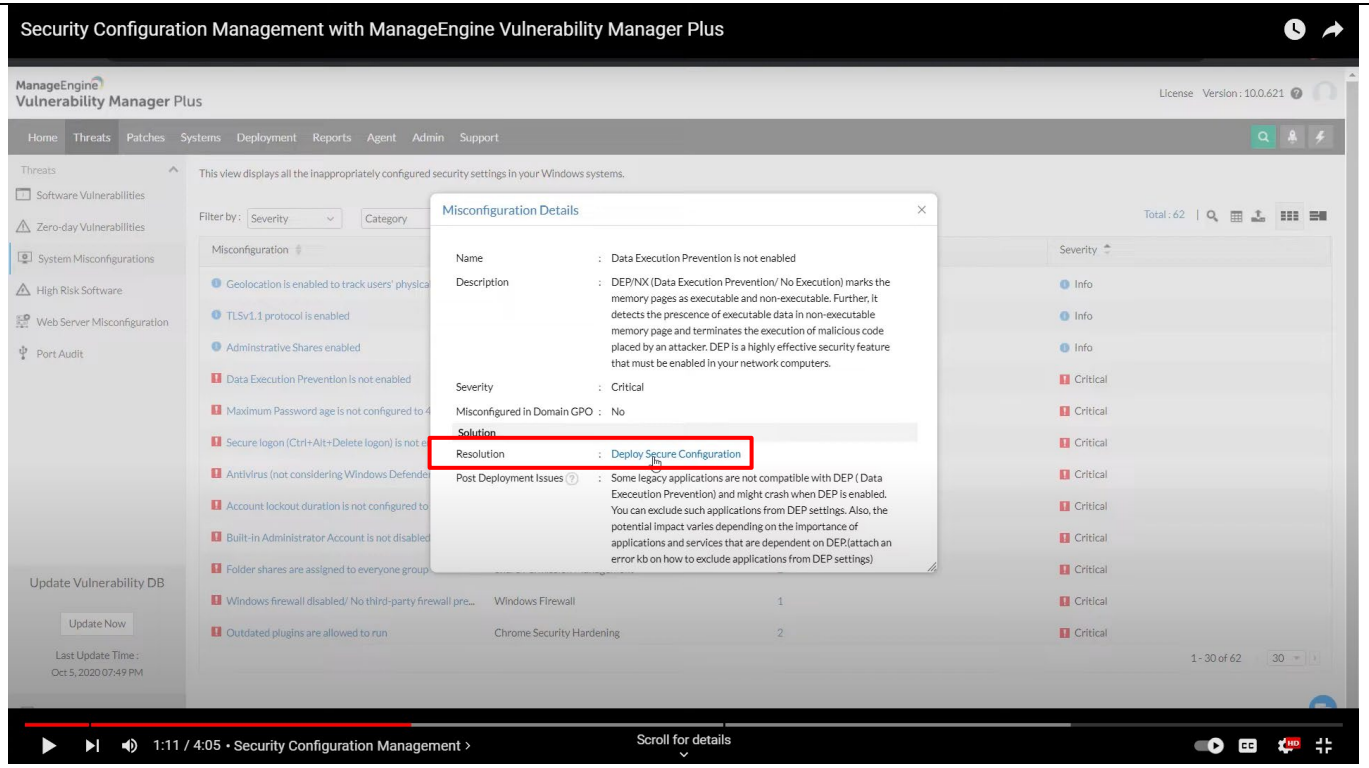
U.S. Patent No 10,075,466 v. Zoho



https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho



https://www.youtube.com/watch?v=p2Oh87NruMo&t=53s

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

	Firewall Policy Management Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes. • Add, modify, and delete network and service objects • Add, modify, and delete firewall rules • Analyze the implications of proposed firewall rule changes • Push changes directly to the firewall Refer the 'Firewall Rule Administration' page for more details. Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for most major firewall devices including Cisco, FortiGate, WatchGuard, and Check Point. https://www.manageengine.com/products/firewall/firewall-rule-management.html

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

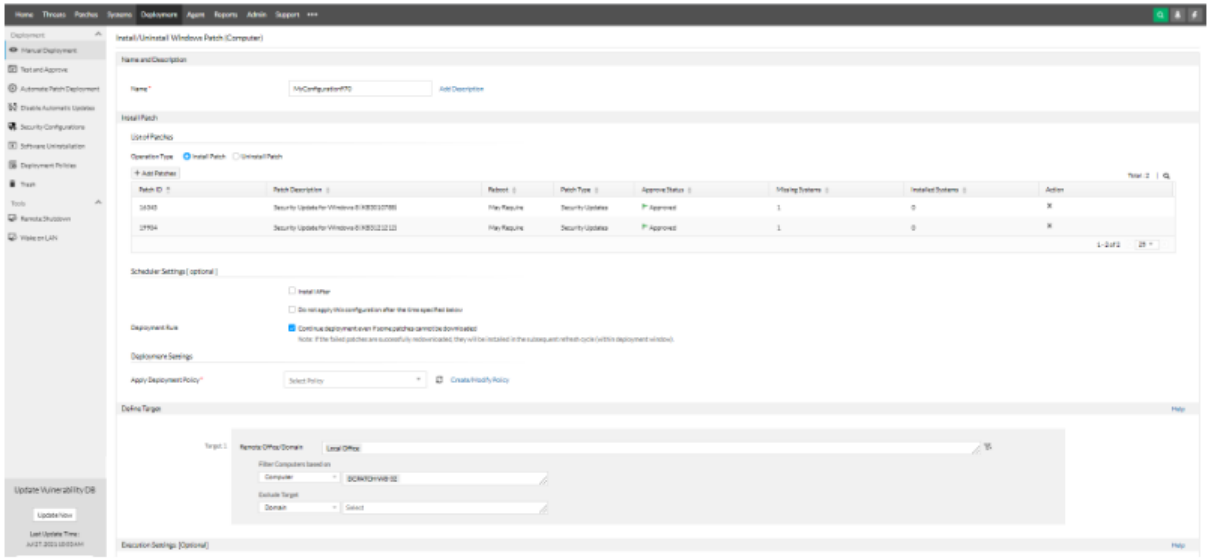
	Leverage built-in patching to ensure swift and accurate remediation With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.  https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html
apply, based on the user input causing selection of the first	ManageEngine *apply, based on the user input causing selection of the first technique for utilizing the intrusion prevention system component for occurrence mitigation, the first technique for utilizing the*

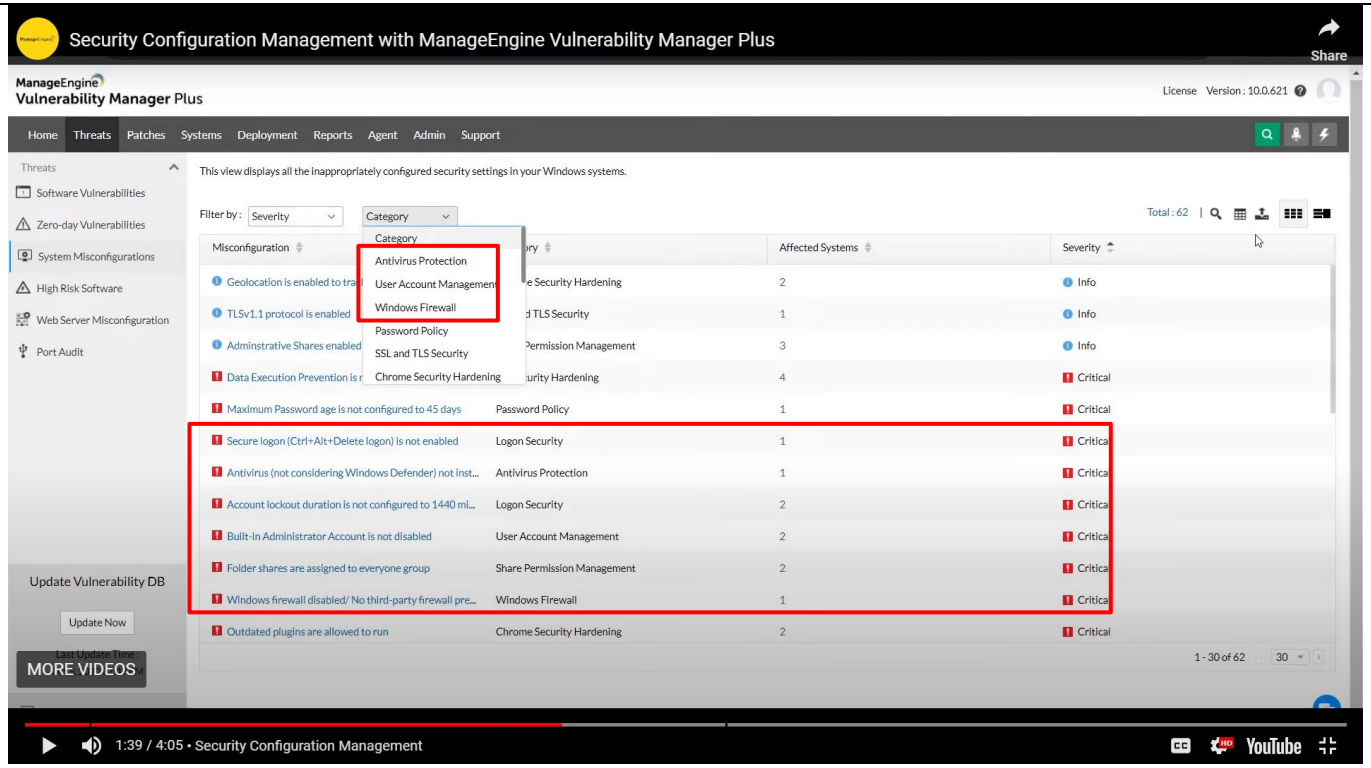
EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

technique for utilizing the intrusion prevention system component for occurrence mitigation, the first technique for utilizing the intrusion prevention system component for occurrence mitigation; apply, based on the user input causing selection of the second technique for utilizing the firewall for occurrence mitigation, the second technique for utilizing the firewall for occurrence mitigation;	*intrusion prevention system component for occurrence mitigation* (e.g., ManageEngine Vulnerability Manager Plus includes web consol on which user can select antivirus option) , *apply, based on the user input causing selection of the second technique for utilizing the firewall for occurrence mitigation, the second technique for utilizing the firewall for occurrence mitigation* (e.g., ManageEngine Vulnerability Manager Plus includes firewall option). The ManageEngine provides flexibility to choose the devices for applying the different policies or mitigation techniques according to the requirements. Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Intrusion detection and prevention** Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules. At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any. https://www.manageengine.com/security.html?mesearch

EXHIBIT 14

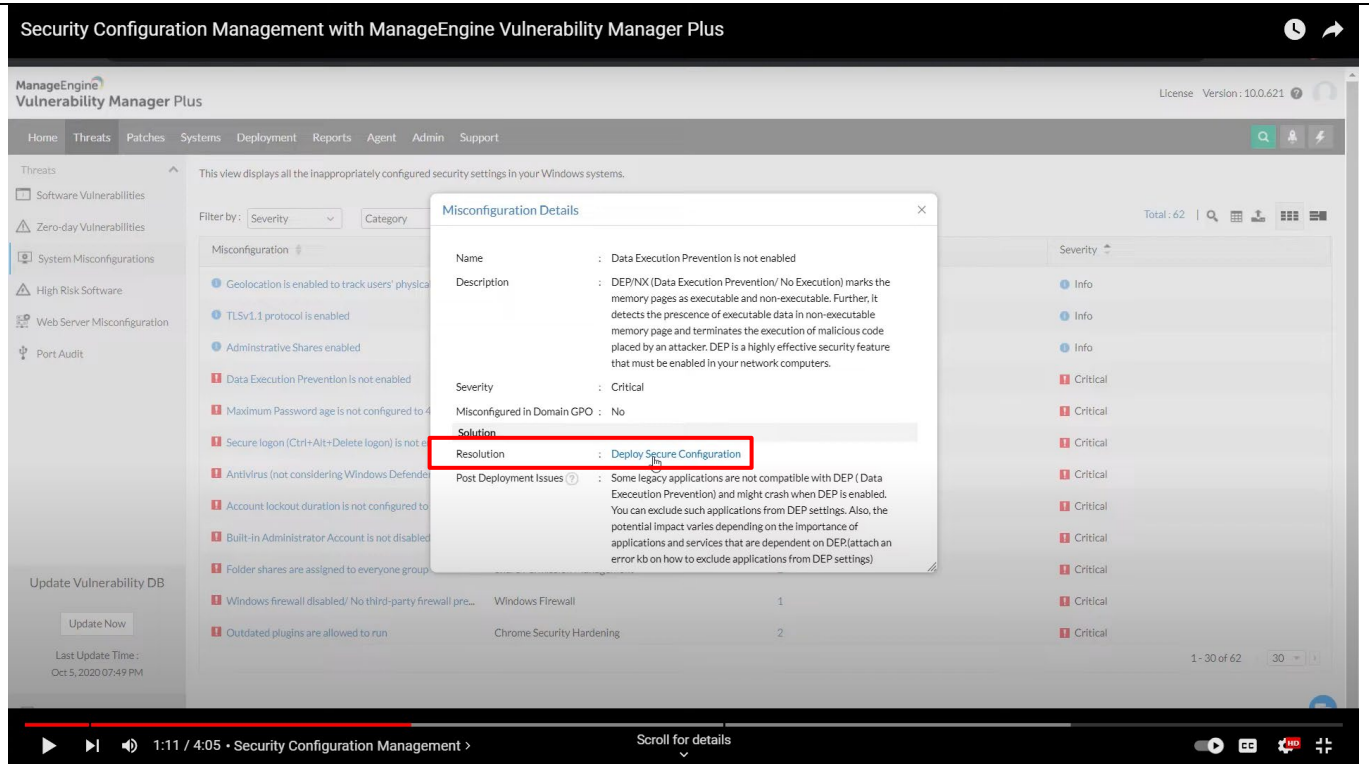
U.S. Patent No 10,075,466 v. Zoho



https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho



https://www.youtube.com/watch?v=p2Oh87NruMo&t=53s

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

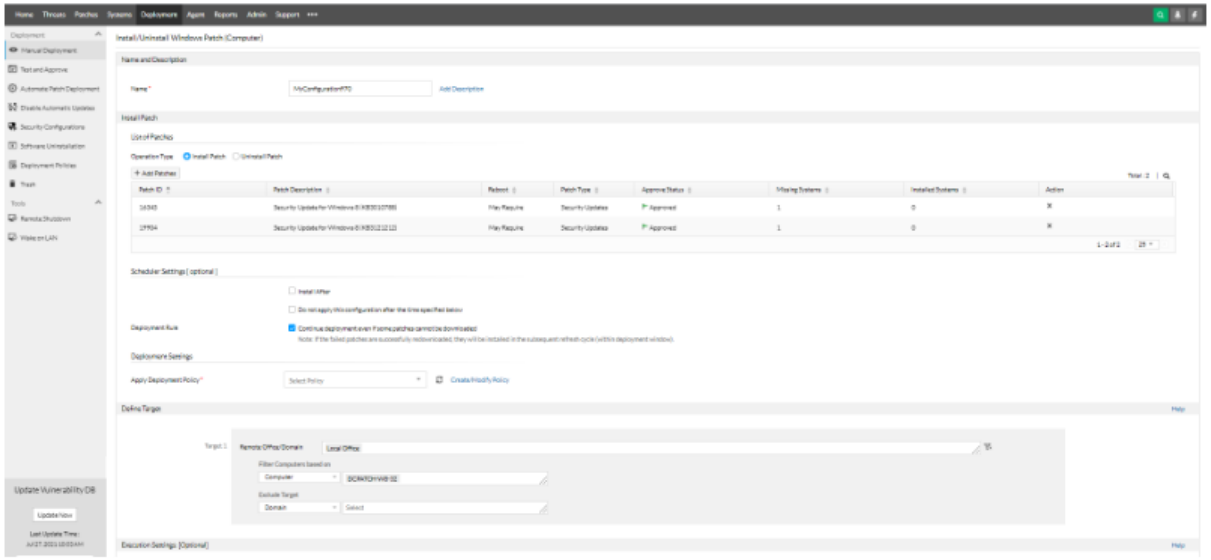
	# Firewall Policy Management Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes. • Add, modify, and delete network and service objects • Add, modify, and delete firewall rules • Analyze the implications of proposed firewall rule changes • Push changes directly to the firewall Refer the 'Firewall Rule Administration' page for more details. Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for most major firewall devices including Cisco, FortiGate, WatchGuard, and Check Point. https://www.manageengine.com/products/firewall/firewall-rule-management.html

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Leverage built-in patching to ensure swift and accurate remediation

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.



https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

identify : for the at least one networked device, a first occurrence including at least one first occurrence packet, and for the at least one networked device, a second occurrence including at least one second occurrence packet;	ManageEngine *identify, for the at least one networked device, a first occurrence including at least one first occurrence packet* (e.g., Bad traffic), *for the at least one networked device, a second occurrence including at least one second occurrence packet* (e.g., good traffic). Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **DDoS prevention** We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our websites, applications, and APIs highly available and performing. https://www.manageengine.com/security.html?mesearch

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

	Intrusion detection and prevention Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules. At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any. https://www.manageengine.com/security.html?mesearch
determine: that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one	ManageEngine *determine, that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable* (e.g., Bad traffic) , *that the second occurrence including the at least one second occurrence packet directed to the at least one networked device is not capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable* (e.g., good traffic). Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

of the actual vulnerability to which the at least one networked device is actually vulnerable; that the second occurrence including the at least one second occurrence packet directed to the at least one networked device is not capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable; and	**DDoS prevention** We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our websites, applications, and APIs highly available and performing. https://www.manageengine.com/security.html?mesearch **Intrusion detection and prevention** Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules. At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any. https://www.manageengine.com/security.html?mesearch

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

cause a reporting of at least the first occurrence based on the determination that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable.	ManageEngine *cause a reporting of at least the first occurrence based on the determination that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable* (e.g., mitigation capabilities to prevent disruptions caused by bad traffic and reported to the user) Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **DDoS prevention** We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our websites, applications, and APIs highly available and performing. https://www.manageengine.com/security.html?mesearch

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

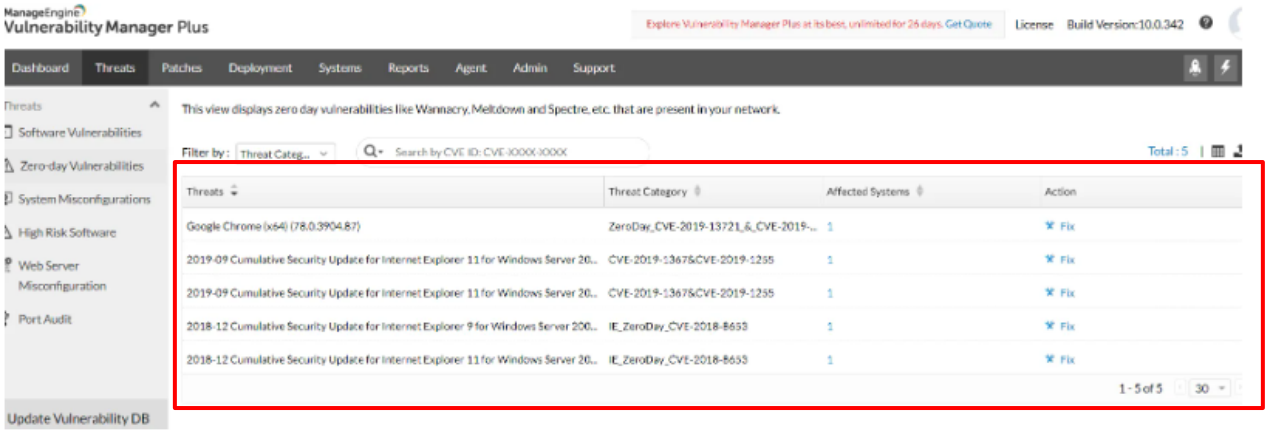
	Intrusion detection and prevention Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules. At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any. https://www.manageengine.com/security.html?mesearch

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Leverage a dedicated view for zero-days

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.



Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network. Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. *Subscribe to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news*

https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

	Incident Management **Reporting** We have a dedicated incident management team. We notify you of the incidents in our environment that apply to you, along with suitable actions that you may need to take. We track and close the incidents with appropriate corrective actions. Whenever applicable, we will identify, collect, acquire and provide you with necessary evidence the form of application and audit logs regarding incidents that apply to you. Furthermore, we implement controls to prevent recurrence of similar situations. We respond to the security or privacy incidents you report to us through incidents@zohocorp.com, with high priority. For general incidents, we will notify users through our blogs, forums, and social media. For incidents specific to an individual user or an organization, we will notify the concerned party through email (using their primary email address of the Organisation administrator registered with us). https://www.manageengine.com/security.html?mesearch